Apple Transparency Report: Government and Private Party Requests

July 1–December 31, 2023

Introduction

Apple is very seriously committed to protecting your data and we work hard to deliver the most secure hardware, software and services available. We believe our customers have a right to understand how their personal data is managed and protected. This report provides information regarding requests Apple received from government agencies worldwide and U.S. private parties from July 1 through December 31, 2023.

Types of requests we receive

Apple receives various forms of legal requests seeking information from or actions by Apple. We receive requests from governments globally where we operate and from private parties.

Government request circumstances can vary from instances where law enforcement agencies are working on behalf of customers who have requested assistance regarding lost or stolen devices, to instances where law enforcement are working on behalf of customers who suspect their credit card has been used fraudulently to purchase Apple products or services, to instances where an account is suspected to have been used unlawfully. Requests can also seek to preserve an Apple account, restrict access to an Apple account or delete an Apple account. Additionally, requests can relate to emergency situations where there is imminent harm to the safety of any person. Apple may also receive requests from government agencies seeking customer data related to specific latitude and longitude coordinates (geofence) for a specified time period. Apple does not have any data to provide in response to geofence requests.

Digital Content Provider government request circumstances generally relate to law enforcement investigations where a service or content (such as an app, music item, or podcast) is suspected to violate local law.

Private party request circumstances generally relate to instances where private litigants are involved in either civil or criminal proceedings.

Types of legal requests Apple receives from the United States can be: subpoenas, court orders, search warrants, pen register/trap and trace orders, or wiretap orders.

Types of legal requests Apple receives internationally can be: Production Orders (Australia, Canada, New Zealand), Requisition or Judicial Rogatory Letters (France), Solicitud Datos (Spain), Ordem Judicial (Brazil), Auskunftsersuchen (Germany), Obligation de dépôt (Switzerland), 個人情報の開示依頼 (Japan), Personal Data Request (United Kingdom), as well as equivalent court orders and/or requests from other countries.

The restrictions imposed by the sanctions laws generally prohibit Apple from responding to requests from countries, territories or governments sanctioned by the U.S. Department of Treasury, with the exception of requests involving exempt informational material or where prior authorization has been secured.

Types of customer data sought in requests

The type of customer data sought in requests varies depending on the case under investigation. For example, in stolen device cases, law enforcement generally seek details of customers associated with devices or device connections to Apple services. In credit card fraud cases, law enforcement generally seek details of suspected fraudulent transactions. Depending on what the legal request asks, Apple will provide subscriber or transaction details in response to valid legal requests received.

In instances where an Apple account is suspected of being used unlawfully, law enforcement may seek details of the customer associated with the account, account connections or transaction details or account content. Any U.S. government agency seeking customer content data from Apple must obtain a search warrant issued upon a showing of probable cause. International requests for content must comply with applicable laws, including the U.S. Electronic Communications Privacy Act (ECPA). A request under a Mutual Legal Assistance Treaty or Agreement with the U.S. is in compliance with ECPA.

The type of customer data sought in emergency situations generally relates to details of customers' connection to Apple services. We have a dedicated team available around the clock to respond to emergency requests. Apple processes emergency requests from law enforcement globally on a 24/7 basis. An emergency request must relate to circumstances involving imminent danger of death or serious physical injury to any person. If Apple believes in good faith that it is a valid emergency, we may voluntarily provide information to law enforcement on an emergency basis.

How we manage and respond to requests

Apple has a centralized and standardized process for receiving, tracking, processing, and responding to legal requests from law enforcement, government, and private parties worldwide, from when a request is received until when a response is provided.

Government and private entities are required to follow applicable laws and statutes when requesting customer information and data. We contractually require our service providers to abide by the same standard for any government information requests for Apple data. Our legal team reviews requests received to ensure that the requests have a valid legal basis. If they do, we comply with the requests and provide data responsive to the request. If we determine a request does not have a valid legal basis, or if we consider it to be unclear, inappropriate and/or over-broad, we challenge or reject it.

How we count requests and responses

Apple counts requests received from government agencies worldwide and United States private parties within the reporting period in which they are received. Overall numbers of requests and responses are reported.

A request with a valid legal basis is processed and responded to, and is counted as one request. A request that is challenged/rejected is counted as one request. Where new legal process is submitted to amend the request, it is counted as a new request. We count each request we challenge or reject for account, account restriction/deletion, emergency, digital content provider, and United States private party requests, and report these numbers accordingly.

We count the number of discernible devices, financial identifiers, accounts and/or push tokens specified in requests, and report these accordingly by type. If there are two identifiers for one device in a request, for example a serial number and IMEI number, we count this as one device. If there are multiple identifiers for one account in a request, for example Apple ID, full name and phone number, we count this as one account.

For United States Government Requests by Legal Process Type reporting, where two types of legal process are combined in a single request, such as a search warrant with an incorporated court order, we record the request at the highest level of legal process and the request would be reported as a search warrant. An exception is where a pen register/trap and trace order is received; this is counted as a pen register/trap and trace order, notwithstanding that it may include a search warrant.

How we report requests and responses

We report on requests and responses in the following categories:

1) Worldwide Government Device Requests
2) Worldwide Government Financial Identifier Requests
3) Worldwide Government Account Requests
4) Worldwide Government Account Preservation Requests
5) Worldwide Government Account Restriction/Deletion Requests
6) Worldwide Government Push Token Requests
7) Worldwide Government Emergency Requests
8) US-UK Data Access Agreement: Warrant Requests from the UK
9) United States Government National Security Requests
10) United States Government Device Requests by Legal Process Type
11) United States Government Financial Identifier Requests by Legal Process Type
12) United States Government Account Requests by Legal Process Type
13) United States Government Push Token Requests by Legal Process Type
14) United States Government Geofence Requests by Legal Process Type
15) United States Private Party Requests for Information
16) United States Private Party Requests for Account Restriction/Deletion
17) Worldwide Government Digital Content Provider Requests

For government agency requests for customer information and data, we report the numbers of requests we receive and our responses in various categories. For United States National Security requests for customer information and data, we report as much detail as we are legally allowed. In order to report FISA non-content and content requests in separate categories, Apple is required by law to delay reporting by 6 months and report the numbers in ranges of 500, pursuant to the USA FREEDOM Act of 2015. For United States-United Kingdom Data Access Agreement (CLOUD) Investigatory Powers Act warrant requests, Apple is required by law to delay reporting by 6 months and report the numbers in ranges of 500, pursuant to 2018 No. 349.

Customer notification

When we receive an account request seeking our customers' information and data, we notify the customer that we have received a request concerning their personal data except where we are explicitly prohibited by the legal process, by a court order Apple receives, or by applicable law. We reserve the right to make exceptions, such as instances where we believe providing notice creates a risk of injury or death to an identifiable individual, or where the case relates to child endangerment, or where notice is not applicable to the underlying facts of the case.

Table 1: Worldwide Government Device Requests
July 1–December 31, 2023

Table 1 provides information regarding device-based requests received. Examples of such requests are where law enforcement agencies are working on behalf of customers who have requested assistance regarding lost or stolen devices. Additionally, Apple regularly receives multi-device requests related to fraud investigations. Device-based requests generally seek details of customers associated with devices or device connections to Apple services.

Country or Region[1]	# of Device Requests Received	# of Devices Specified in the Requests	# of Device Requests Where Data Provided	% of Device Requests Where Data Provided
Asia Pacific				
Australia	486	1,403	193	40%
China mainland	905	42,762	853	94%
Hong Kong	15	137	5	33%
Japan	207	432	119	57%
Malaysia	1	10	1	100%
New Zealand	15	17	3	20%
Philippines	1	1	0	0%
Singapore	630	651	367	58%
South Korea	40	178	26	65%
Taiwan	40	85	31	78%
Thailand	10	25	1	10%
Vietnam	2	44	0	0%
Asia Pacific Total	2,352	45,745	1,599	68%
Europe, Middle East, India, Africa				
Andorra	3	4	0	0%
Austria	36	62	5	14%
Azerbaijan	1	3	0	0%
Belgium	70	141	41	59%
Bulgaria	2	3	0	0%
Croatia	3	4	3	100%
Czech Republic	73	105	50	68%
Denmark	6	18	2	33%
Finland	11	45	3	27%
France	710	1,599	305	43%
Germany	8,866	16,533	4,463	50%
Greece	6	8	0	0%
Hungary	21	45	7	33%
India	121	3,138	17	14%
Ireland	25	112	16	64%
Israel	9	10	5	56%
Italy	195	7,319	12	6%
Kosovo	1	2	0	0%
Luxembourg	3	37	1	33%
Malta	1	2	1	100%
Netherlands	67	4,592	39	58%
Norway	5	12	1	20%
Pakistan	1	1	0	0%
Poland	68	2,563	17	25%
Portugal	44	60	6	14%
Qatar	1	1	1	100%
Romania	8	12	3	38%
Russia	16	23	0	0%
Slovakia	1	18	0	0%
Slovenia	6	7	5	83%
South Africa	5	27	2	40%
Spain	620	1,098	290	47%
Sweden	87	123	66	76%
Switzerland	56	4,959	15	27%
Türkiye	56	60	4	7%
Ukraine	11	2,498	0	0%
United Arab Emirates	2	2	0	0%
United Kingdom	1,633	2,197	1,337	82%
Europe, Middle East, India, Africa Total	12,850	47,443	6,717	52%
Latin America				
Argentina	9	21	1	11%
Brazil	5,858	20,101	4,765	81%
Chile	122	153	65	53%
Colombia	2	2	0	0%
Costa Rica	1	2	1	100%
Ecuador	2	2	0	0%
Honduras	1	1	0	0%
Latin America Total	5,995	20,282	4,832	81%

[1] Only countries / regions where Apple received device requests during report period July 1–December 31, 2023 are listed.

Table 1: Worldwide Government Device Requests (continued)
July 1–December 31, 2023

Table 1 provides information regarding device-based requests received. Examples of such requests are where law enforcement agencies are working on behalf of customers who have requested assistance regarding lost or stolen devices. Additionally, Apple regularly receives multi-device requests related to fraud investigations. Device-based requests generally seek details of customers associated with devices or device connections to Apple services.

Country or Region[1]	# of Device Requests Received	# of Devices Specified in the Requests	# of Device Requests Where Data Provided	% of Device Requests Where Data Provided
North America				
Canada	76	131	65	86%
Mexico	8	12	2	25%
United States of America	6,410	19,669	5,233	82%
North America Total	6,494	19,812	5,300	82%
Worldwide Total	27,691	133,282	18,448	67%

[1] Only countries / regions where Apple received device requests during report period July 1–December 31, 2023 are listed.

# of Device Requests Received

The number of device-based requests received from a government agency seeking customer data related to specific device identifiers, such as serial number or IMEI number. Requests can be in various formats such as subpoenas, court orders, warrants, or other valid legal requests. We count each individual request received from each country/region and report the total number of requests received by country/region.

# of Devices Specified in the Requests

The number of devices specified in the requests. One request may contain one or multiple device identifiers. For example, in a case related to the theft of a shipment of devices, law enforcement may seek information related to several device identifiers in a single request. We count the number of devices identified in each request, received from each country/region, and report the total number of devices specified in requests received by country/region.

# of Device Requests Where Data Provided

The number of device-based requests that resulted in Apple providing data, such as customers associated with devices, device connections to Apple services, purchase, customer service, or repair information, in response to a valid legal request. We count each device-based request where we provide data and report the total number of such instances by country/region.

% of Device Requests Where Data Provided

The percentage of device-based requests that resulted in Apple providing data. We calculate this based on the number of device-based requests that resulted in Apple providing data per country/region, compared to the total number of device-based requests Apple received from that country/region.

Table 2: Worldwide Government Financial Identifier Requests July 1–December 31, 2023

Table 2 provides information regarding financial identifier-based requests received. Examples of such requests are where law enforcement agencies are working on behalf of customers who have requested assistance regarding suspected fraudulent credit card activity used to purchase Apple products or services. Financial identifier-based requests generally seek details of suspected fraudulent transactions.

Country or Region[1]	# of Financial Identifier Requests Received	# of Financial Identifiers Specified in the Requests	# of Financial Identifier Requests Where Data Provided	% of Financial Identifier Requests Where Data Provided
Asia Pacific				
Australia	92	326	32	35%
China mainland	327	6,810	278	85%
Hong Kong	296	447	113	38%
Japan	477	3,049	300	63%
Macau	33	112	15	45%
New Zealand	1	1	1	100%
Singapore	435	2,919	287	66%
South Korea	154	1,786	131	85%
Taiwan	4,415	57,604	4,345	98%
Thailand	14	15	3	21%
Asia Pacific Total	6,244	73,069	5,505	88%
Europe, Middle East, India, Africa				
Andorra	1	20	0	0%
Austria	74	543	8	11%
Azerbaijan	2	2	0	0%
Belgium	9	33	3	33%
Croatia	1	1	1	100%
Czech Republic	7	21	3	43%
Denmark	1	57	1	100%
Finland	15	85	8	53%
France	259	835	139	54%
Germany	982	3,818	547	56%
Greece	6	10	0	0%
Hungary	133	136	43	32%
India	171	1,881	23	13%
Ireland	36	302	22	61%
Israel	5	9	5	100%
Italy	219	847	20	9%
Jordan	2	2	0	0%
Lebanon	1	1	0	0%
Lithuania	2	2	0	0%
Luxembourg	4	29	0	0%
Moldova	1	1	0	0%
Netherlands	7	21	2	29%
Norway	3	10	3	100%
Poland	50	287	13	26%
Portugal	39	237	14	36%
Romania	46	47	18	39%
Russia	1	3	0	0%
San Marino	1	15	1	100%
Serbia	1	1	1	100%
Slovakia	3	24	1	33%
Slovenia	1	1	0	0%
Spain	593	1,050	197	33%
Sweden	14	308	8	57%
Switzerland	75	418	50	67%
Türkiye	449	459	147	33%
Ukraine	1	1	0	0%
United Arab Emirates	2	2	0	0%
United Kingdom	104	214	4	4%
Europe, Middle East, India, Africa Total	3,321	11,733	1,282	39%
Latin America				
Argentina	3	3	0	0%
Brazil	6	45	4	67%
Chile	1	1	0	0%
Costa Rica	5	5	1	20%
Dominican Republic	1	1	0	0%
Latin America Total	16	55	5	31%

[1] Only countries / regions where Apple received financial identifier requests during report period July 1–December 31, 2023 are listed.

Table 2: Worldwide Government Financial Identifier Requests (continued)
July 1–December 31, 2023

Table 2 provides information regarding financial identifier-based requests received. Examples of such requests are where law enforcement agencies are working on behalf of customers who have requested assistance regarding suspected fraudulent credit card activity used to purchase Apple products or services. Financial identifier-based requests generally seek details of suspected fraudulent transactions.

Country or Region[1]	# of Financial Identifier Requests Received	# of Financial Identifiers Specified in the Requests	# of Financial Identifier Requests Where Data Provided	% of Financial Identifier Requests Where Data Provided
North America				
Canada	19	61	17	89%
Mexico	1	1	0	0%
United States of America	1,018	3,563	744	73%
North America Total	1,038	3,625	761	73%
Worldwide Total	10,619	88,482	7,553	71%

[1] Only countries / regions where Apple received financial identifier requests during report period July 1–December 31, 2023 are listed.

# of Financial Identifier Requests Received

The number of financial identifier-based requests received from a government agency seeking customer data related to specific financial identifiers, such as credit card or gift card number. Financial identifier-based requests can be in various formats such as subpoenas, court orders, warrants, or other valid legal requests. We count each individual request received from each country/region and report the total number of requests received by country/region.

# of Financial Identifiers Specified in the Requests

The number of financial identifiers specified in the requests. One request may contain one or multiple financial identifiers. For example, in a case related to large scale fraud, law enforcement may seek information related to several credit card numbers in a single request. We count the number of financial identifiers identified in each request, received from each country/region, and report the total number of financial identifiers specified in requests received by country/region.

# of Financial Identifier Requests Where Data Provided

The number of financial identifier-based requests that resulted in Apple providing data, such as transaction details, in response to a valid legal request. We count each financial identifier-based request where we provide data and report the total number of such instances by country/region.

% of Financial Identifier Requests Where Data Provided

The percentage of financial identifier-based requests that resulted in Apple providing data. We calculate this based on the number of financial identifier-based requests that resulted in Apple providing data per country/region, compared to the total number of financial identifier-based requests Apple received from that country/region.

Table 3: Worldwide Government Account Requests
July 1–December 31, 2023

Table 3 provides information regarding account-based requests received. Examples of such requests are where law enforcement agencies are working on cases where they suspect an account may have been used unlawfully or in violation of Apple's terms of service. Account-based requests generally seek details of customers' iTunes or iCloud accounts, such as a name and address; and in certain instances customers' iCloud content, such as stored photos, email, iOS device backups, contacts or calendars.

Country or Region[1]	# of Account Requests Received	# of Accounts Specified in the Requests	# of Account Requests Challenged in Part or Rejected in Full	# of Account Requests Where Only Non-Content Data Provided	# of Account Requests Where Content Data Provided	% of Account Requests Where Data Provided
Asia Pacific						
Australia	273	370	32	155	0	57%
China mainland	191	772	9	94	41	71%
Hong Kong	10	12	1	9	0	90%
Japan	259	482	79	141	1	55%
Macau	1	1	0	0	0	0%
New Zealand	6	10	2	3	0	50%
Philippines	2	2	1	0	0	0%
Singapore	51	63	4	27	0	53%
South Korea	55	65	0	40	0	73%
Taiwan	187	363	5	159	0	85%
Thailand	1	1	1	0	0	0%
Asia Pacific Total	1,036	2,141	134	628	42	65%
Europe, Middle East, India, Africa						
Albania	1	1	1	0	0	0%
Austria	58	73	47	6	0	10%
Belgium	55	64	1	42	0	76%
Croatia	1	1	0	0	1	100%
Czech Republic	169	249	9	149	1	89%
Denmark	5	5	2	3	0	60%
Finland	17	26	0	14	0	82%
France	456	1,021	39	294	2	65%
Germany	1,925	2,463	294	1,217	3	63%
Greece	5	7	5	0	0	0%
Hungary	51	59	18	18	0	35%
India	86	137	75	4	0	5%
Ireland	32	45	8	15	1	50%
Israel	15	19	1	12	0	80%
Italy	145	151	48	36	0	25%
Kosovo	1	1	1	0	0	0%
Latvia	1	1	0	1	0	100%
Liechtenstein	1	4	1	0	0	0%
Lithuania	2	2	1	1	0	50%
Malta	4	4	1	1	0	25%
Netherlands	56	164	6	39	1	71%
Norway	2	2	1	0	0	0%
Pakistan	1	1	1	0	0	0%
Poland	75	106	55	8	0	11%
Portugal	8	11	6	1	0	13%
Qatar	1	1	0	1	0	100%
Romania	13	28	4	5	0	38%
Russia	8	12	7	0	0	0%
South Africa	1	2	1	0	0	0%
Spain	101	135	33	34	0	34%
Sweden	268	319	5	224	0	84%
Switzerland	52	115	12	24	2	50%
Türkiye	41	42	23	12	0	29%
Ukraine	1	1	0	0	0	0%
United Kingdom	1,414	1,617	41	1,142	1	81%
Europe, Middle East, India, Africa Total	5,072	6,889	747	3,303	12	65%

[1] Only countries / regions where Apple received account requests during report period July 1–December 31, 2023 are listed.

Table 3: Worldwide Government Account Requests (continued)
July 1–December 31, 2023

Table 3 provides information regarding account-based requests received. Examples of such requests are where law enforcement agencies are working on cases where they suspect an account may have been used unlawfully or in violation of Apple's terms of service. Account-based requests generally seek details of customers' iTunes or iCloud accounts, such as a name and address; and in certain instances customers' iCloud content, such as stored photos, email, iOS device backups, contacts or calendars.

Country or Region[1]	# of Account Requests Received	# of Accounts Specified in the Requests	# of Account Requests Challenged in Part or Rejected in Full	# of Account Requests Where Only Non-Content Data Provided	# of Account Requests Where Content Data Provided	% of Account Requests Where Data Provided
Latin America						
Argentina	7	10	5	1	0	14%
Belize	1	1	1	0	0	0%
Brazil	3,327	16,741	581	605	1,754	71%
Chile	18	19	4	7	0	39%
Colombia	4	12	4	0	0	0%
Costa Rica	7	7	0	5	0	71%
Ecuador	4	14	4	0	0	0%
Peru	1	6	1	0	0	0%
Latin America Total	3,369	16,810	600	618	1,754	70%
North America						
Canada	89	157	9	79	2	91%
Mexico	12	23	7	3	0	25%
United States of America	10,827	32,529	1,394	4,786	4,981	90%
North America Total	10,928	32,709	1,410	4,868	4,983	90%
Worldwide Total	20,405	58,549	2,891	9,417	6,791	79%

[1] Only countries / regions where Apple received account requests during report period July 1–December 31, 2023 are listed.

# of Account Requests Received

The number of account-based requests received from a government agency seeking customer data related to specific Apple account identifiers, such as Apple ID or email address. Account-based requests can be in various formats such as subpoenas, court orders, warrants, or other valid legal requests. We count each individual request received from each country/region and report the total number of requests received by country/region.

# of Accounts Specified in the Requests

The number of accounts specified in the requests. One request may contain one or multiple account identifiers. For example, in a case related to suspected phishing, law enforcement may seek information related to several accounts in a single request. We count the number of accounts identified in each request, received from each country/region, and report the total number of accounts specified in requests received by country/region.

# of Account Requests Challenged in Part or Rejected in Full

The number of account-based requests that resulted in Apple challenging the request in part, or rejecting the request in full, based on grounds such as a request does not have a valid legal basis, or is unclear, inappropriate, and/or over-broad. For example, Apple may reject a law enforcement request if it considers the scope of data requested as excessively broad for the case in question. We count each account-based request where we challenge it in part, or reject it in full, and report the total number of such instances by country/region.

# of Account Requests Where Only Non-Content Data Provided

The number of account-based requests that resulted in Apple only providing non-content data, such as subscriber, account connections or transactional information, in response to a valid legal request. We count each account-based request where we provide only non-content data and report the total number of such instances by country/region.

# of Account Requests Where Content Data Provided

The number of account-based requests that resulted in Apple providing content data, such as stored photos, email, iOS device backups, contacts or calendars, in response to a valid legal request. We count each account-based request where we provide content data and report the total number of such instances by country/region.

% of Account Requests Where Data Provided

The percentage of account-based requests that resulted in Apple providing either non-content and/or content data. We calculate this based on the number of account-based requests that resulted in Apple providing data (including both non-content and content) per country/region, compared to the total number of account-based requests Apple received from that country/region.

Table 4: Worldwide Government Account Preservation Requests July 1–December 31, 2023

Table 4 provides information regarding account preservation requests received. Under the U.S. Electronic Communications Privacy Act (ECPA), government agencies may request Apple to preserve users' account data by performing a one-time data pull of the requested existing user data available at the time of the request for 90 days (up to 180 days if Apple receives a renewal request). Examples of such requests are where law enforcement agencies suspect an account may have been used unlawfully or in violation of Apple's terms of service, and request Apple to preserve the account data while they obtain legal process for the data.

Country or Region[1]	# of Account Preservation Requests Received	# of Accounts Specified in the Requests	# of Accounts Where Data Preserved
Asia Pacific			
Australia	6	7	5
New Zealand	9	11	11
South Korea	1	1	0
Asia Pacific Total	16	19	16
Europe, Middle East, India, Africa			
Austria	4	4	3
Belgium	4	5	5
Bosnia and Herzegovina	2	2	2
Czech Republic	1	2	0
Denmark	7	7	7
Finland	4	13	6
France	2	7	6
Germany	53	71	61
Ireland	10	13	13
Israel	1	1	1
Italy	1	1	1
Kosovo	2	5	5
Netherlands	5	20	17
Norway	1	5	3
Poland	1	1	1
Romania	1	1	1
Slovenia	2	2	2
Spain	1	1	1
Sweden	7	40	33
Switzerland	2	3	3
Türkiye	1	2	2
Ukraine	2	14	10
United Kingdom	47	71	54
Europe, Middle East, India, Africa Total	161	291	237
Latin America			
Brazil	242	953	466
Guatemala	1	4	0
Latin America Total	243	957	466
North America			
Canada	57	89	79
Mexico	5	6	4
United States of America	6,610	21,321	16,682
North America Total	6,672	21,416	16,765
Worldwide Total	7,092	22,683	17,484

[1] Only countries / regions where Apple received account preservation requests during report period July 1–December 31, 2023 are listed.

# of Account Preservation Requests Received

The number of account preservation requests received from a government agency. We count each individual request received from each country/region and report the total number of requests received by country/region.

# of Accounts Specified in the Requests

The number of accounts specified in the requests. One request may contain one or multiple account identifiers. For example, in a case related to suspected illegal activity, law enforcement may request Apple to preserve information related to several accounts in a single request. We count the number of accounts identified in each request, received from each country/region, and report the total number of accounts specified in requests received by country/region.

# of Accounts Where Data Preserved

The number of accounts that resulted in Apple preserving data in response to a valid preservation request. We count the number of accounts in each request where data was preserved and report the total number of accounts for which data was preserved by country/region.

Table 5: Worldwide Government Account Restriction/Deletion Requests July 1–December 31, 2023

Table 5 provides information regarding account restriction/deletion requests received. Examples of such requests are where law enforcement agencies suspect an account may have been used unlawfully or in violation of Apple's terms of service, and request Apple to restrict or delete the account. For requests seeking to restrict/delete a customer's Apple ID, Apple requires a court order (including conviction or warrant) demonstrating that the account to be restricted/deleted was used unlawfully, except in situations where the case has been verified by Apple to relate to child endangerment.

Country or Region[1]	# of Account Restriction/ Account Deletion Requests Received	# of Accounts Specified in the Requests	# of Requests Rejected/ Challenged Where No Action Taken	# of Requests Where Account Restricted	# of Requests Where Account Deleted
Asia Pacific					
Japan	1	1	0	1	0
Asia Pacific Total	1	1	0	1	0
Europe, Middle East, India, Africa					
Germany	13	14	2	11	0
Italy	1	1	0	1	0
Netherlands[2]	7	16	1	5	0
Norway	1	1	0	1	0
Pakistan	1	1	0	1	0
United Kingdom	3	3	0	3	0
Europe, Middle East, India, Africa Total	26	36	3	22	0
Latin America					
-	0	0	0	0	0
Latin America Total	0	0	0	0	0
North America					
Canada [3,4]	8	8	0	5	0
United States of America [2,3]	31	43	3	26	0
North America Total	39	51	3	31	0
Worldwide Total	66	88	6	54	0

[1] Only countries / regions where Apple received account restriction/deletion requests during report period July 1–December 31, 2023 are listed.
[2] One request received where Apple had no results for the account(s) identified in the request.
[3] One request received where Apple Account was in inactive state prior to when the request was received.
[4] Two requests received where Apple had no results for the account(s) identified in the request.

# of Account Restriction/Account Deletion Requests Received	The number of requests received from a government agency seeking to restrict or delete a customer's Apple account. We count each individual request received from each country/region and report the total number of requests received by country/region.
# of Accounts Specified in the Requests	The number of accounts specified in the requests. One request may contain one or multiple account identifiers. For example, in a case related to possession or distribution of illegal material, law enforcement may request Apple to restrict or delete several accounts in a single request. We count the number of accounts identified in each request, received from each country/region, and report the total number of accounts specified in requests received by country/region.
# of Requests Rejected/ Challenged Where No Action Taken	The number of account restriction/deletion requests that resulted in Apple challenging or rejecting the request based on grounds such as a request does not have a valid legal basis, or is unclear, inappropriate, and/or over-broad, or where it is not accompanied by a court order (including conviction or warrant) demonstrating that the account to be restricted/deleted was used unlawfully; and where no action was taken by Apple. We count each account restriction/ deletion request where we challenge or reject it and report the total number of such instances by country/region.
# of Requests Where Account Restricted	The number of requests where Apple determined the request and order sufficiently demonstrated the account to be restricted was used unlawfully and we proceeded with restriction. We count each request where we proceeded with account restriction and report the total number of such instances by country/region.
# of Requests Where Account Deleted	The number of requests where Apple determined the request and order sufficiently demonstrated the account to be deleted was used unlawfully and we deleted the Apple account. We count each request where we deleted an account and report the total number of such instances by country/ region.

Table 6: Worldwide Government Push Token Requests July 1–December 31, 2023

When users allow a currently installed application to receive notifications, an Apple Push Notification service token (push token) is generated and registered to that developer and device. Table 6 provides information regarding push token-based requests received. Examples of such requests are where law enforcement agencies are working on cases where they suspect the associated Apple Account may have been used unlawfully. Push token-based requests generally seek identifying details of the Apple Account associated with the device's push token, such as name, physical address and email address.

Country or Region[1]	# of Push Token Requests Received	# of Push Tokens Specified in the Requests	# of Push Token Requests Where Data Provided	% of Push Token Requests Where Data Provided
Asia Pacific				
-	-	-	-	-
Asia Pacific Total	0	0	0	-
Europe, Middle East, India, Africa				
France	1	1	0	0%
Germany	7	11	5	71%
Israel	1	694	0	0%
Netherlands	1	1	0	0%
United Kingdom	123	128	111	90%
Europe, Middle East, India, Africa Total	133	835	116	87%
Latin America				
-	-	-	-	-
Latin America Total	0	0	0	-
North America				
United States of America	99	345	65	66%
North America Total	99	345	65	66%
Worldwide Total	232	1180	181	78%

[1]Only countries / regions where Apple received push token requests during report period July 1–December 31, 2023 are listed.

# of Push Token Requests Received

The number of requests received from a government agency seeking customer data related to specific Apple Push Notification service token identifiers (push token). We count each individual request received from each country/region and report the total number of requests received by country/region.

# of Push Tokens Specified in the Requests

The number of push tokens specified in the requests. One request may contain one or multiple push token identifiers. For example, in a criminal investigation, law enforcement may seek information related to several push tokens in a single request. We count the number of push tokens identified in each request, received from each country/region, and report the total number of push tokens specified in requests received by country/region.

# of Push Token Requests Where Data Provided

The number of push token-based requests that resulted in Apple providing data. We count each push token-based request where we provide data and report the total number of such instances by country/region.

% of Push Token Requests Where Data Provided

The percentage of push token-based requests that resulted in Apple providing data. We calculate this based on the number of push token-based requests that resulted in Apple providing data per country/region, compared to the total number of push token-based requests Apple received from that country/region.

Table 7: Worldwide Government Emergency Requests
July 1–December 31, 2023

Table 7 provides information regarding emergency requests received. Under the U.S. Electronic Communications Privacy Act (ECPA), government agencies may request Apple to voluntarily disclose information, including customer information and contents of communications, to a government entity if Apple believes in good faith that an emergency involving imminent danger of death or serious physical injury to any person requires such disclosure without delay. International agencies may make similar requests to Apple under applicable local law. Examples of such requests are where a person may be missing and law enforcement believes the person may be in danger. Emergency requests generally seek details of customers' connections to Apple services.

Country or Region[1]	# of Emergency Requests Received	# of Requests Rejected/ Challenged & No Data Provided	# of Emergency Requests Where No Data Provided	# of Emergency Requests Where Data Provided	% of Emergency Requests Where Data Provided
Asia Pacific					
Australia	31	6	6	19	61%
China mainland	8	7	0	1	13%
Japan	259	28	16	215	83%
New Zealand	7	1	2	4	57%
Singapore	1	1	0	0	0%
South Korea	3	0	0	3	100%
Asia Pacific Total	309	43	24	242	78%
Europe, Middle East, India, Africa					
Austria	5	1	0	4	80%
Belgium	4	4	0	0	0%
Bulgaria	1	0	0	1	100%
Czech Republic	1	0	0	1	100%
Denmark	1	0	0	1	100%
Finland	4	0	2	2	50%
France	46	15	5	26	57%
Germany	99	13	13	73	74%
Greece	1	0	0	1	100%
India	28	17	2	9	32%
Ireland	1	0	0	1	100%
Israel	52	2	1	49	94%
Italy	18	4	2	12	67%
Libya	2	0	1	1	50%
Netherlands	25	9	3	13	52%
North Macedonia	1	0	0	1	100%
Norway	3	0	1	2	67%
Poland	5	2	1	2	40%
Portugal	4	2	0	2	50%
Slovenia	2	1	1	0	0%
South Africa	4	3	0	1	25%
Spain	5	1	1	3	60%
Sweden	18	5	2	11	61%
Switzerland	32	4	4	24	75%
United Kingdom	655	27	31	597	91%
Europe, Middle East, India, Africa Total	1,017	110	70	837	82%
Latin America					
Brazil	132	38	12	82	62%
Chile	6	4	1	1	17%
Colombia	22	7	2	13	59%
Costa Rica	1	0	0	1	100%
Ecuador	11	3	5	3	27%
Latin America Total	172	52	20	100	58%
North America					
Canada	147	10	12	125	85%
Mexico	1	0	1	0	0%
United States of America	636	106	79	451	71%
North America Total	784	116	92	576	73%
Worldwide Total	2,282	321	206	1755	77%

[1] Only countries / regions where Apple received emergency requests during report period July 1–December 31, 2023 are listed.

# of Emergency Requests Received	The number of emergency requests received from a government agency. We count each individual request received from each country/region and report the total number of requests received by country/region.
# of Requests Rejected/Challenged & No Data Provided	The number of emergency requests that resulted in Apple challenging or rejecting the request based on grounds such as a request is unclear, inappropriate, or fails to demonstrate that it relates to an emergency circumstance; and where no data was provided. We count each emergency request where we challenge or reject it and report the total number of such instances by country/region.
# of Emergency Requests Where No Data Provided	The number of emergency requests that resulted in Apple providing no data. For example, instances where there was no responsive data. We count each emergency request where we do not provide data and report the total number of such instances by country/region.
# of Emergency Requests Where Data Provided	The number of emergency requests that resulted in Apple providing data, such as connections to Apple services, subscriber or transactional information, or in certain instances customers' iCloud content, such as stored photos, email, iOS device backups, contacts or calendars, in response to a valid emergency request. We count each emergency request where we provide data and report the total number of such instances by country/region.
% of Emergency Requests Where Data Provided	The percentage of emergency requests that resulted in Apple providing data. We calculate this based on the number of emergency requests that resulted in Apple providing data per country/region, compared to the total number of emergency requests Apple received from that country/region.

Table 8: US-UK Data Access Agreement: Warrant Requests from the UK July 1–December 31, 2023

Table 8 provides information regarding Investigatory Powers Act ("IPA") warrant requests Apple received from the United Kingdom pursuant to the US-UK Data Access Agreement (entered into force on October 3, 2022).

We report these requests received for Apple Accounts within ranges permissible by law pursuant to The Investigatory Powers (Disclosure of Statistical Information) Regulations 2018 ("IP DSI 2018"). Apple is required by law to delay initial reporting for a period of 18 months and report in bands of 500. Apple is required for subsequent reporting periods to delay reporting by 6 months and report in bands of 500. Though we want to be more specific, this is currently the range permitted under IP DSI 2018 for reporting this level of detail regarding IPA warrant requests received under the US-UK Data Access Agreement. Under the law, Apple is limited in its ability to disclose what information or data may be sought through these requests.

Request Type	# of Requests Received	# of Users/Accounts
IPA Content Requests	500–999	500–999

Request Type

IPA warrant requests issued pursuant to the US-UK Data Access Agreement for content and non-content data. Non-content data is data such as subscriber or transactional information and connection logs. Content data is iCloud data such as stored photos, email, iOS device backups, contacts or calendars.

# of Requests Received

The number of IPA warrant requests received. We count each individual request received for Apple users/accounts and report the total number of requests received within bands/ranges permissible by law. Pursuant to IP DSI 2018, we are limited to providing this data in bands of 500.

# of Users/Accounts

We count the number of users/accounts in each IPA warrant request received for which Apple has data and report the total number of users/accounts within bands permissible by law. Pursuant to IP DSI 2018, we are limited to providing this data in bands of 500.

Table 9: United States Government National Security Requests July 1–December 31, 2023

Table 9 provides information regarding United States national security requests that Apple received for customer data, including orders received under the Foreign Intelligence Surveillance Act ("FISA") and National Security Letters ("NSLs"). To date, Apple has not received any orders for bulk data.

We report national security requests received for Apple users/accounts (NSLs and orders received under FISA) within ranges permissible by law pursuant to the USA FREEDOM Act of 2015 ("USA Freedom"). In order to report FISA non-content and content requests in separate categories, Apple is required by law to delay reporting by 6 months and report in bands of 500. Though we want to be more specific, this is currently the range permitted under USA Freedom for reporting this level of detail regarding national security requests. Apple responds to National Security FISA content requests with information obtained from iCloud. Under the law, Apple cannot further disclose what information or data may be sought through these requests.

National Security Request Type	# of Requests Received	# of Users/Accounts
FISA Non-Content Requests	500–999	37,500–37,999
FISA Content Requests	500–999	56,500–56,999
National Security Letters	0–499	1,000–1,499

National Security Letters where non-disclosure order lifted	0

National Security Request Type

FISA Non-Content & Content Requests: FISA Court-issued orders for non-content or content data. Non-content data is data such as subscriber or transactional information and connection logs. Content data is data such as stored photos, email, iOS device backups, contacts or calendars.

National Security Letters: Federal Bureau of Investigation-issued requests for non-content data in national security investigations. Non-content data is data such as subscriber data. Apple does not produce transactional information and connection logs in response to National Security Letters.

# of Requests Received

The number of United States National Security requests received. We count each individual order and National Security Letter received for Apple users/accounts and report the total number of orders and National Security Letters received within bands/ranges permissible by law. Pursuant to USA Freedom, to report the number of non-content and content orders received, we are limited to providing this data in bands of 500.

# of Users/Accounts

We count the number of users/accounts in each request received for which Apple has data and report the total number of users/accounts within bands permissible by law. Pursuant to USA Freedom, we are limited to providing this data in bands of 500.

Tables 10, 11, 12, 13, 14: United States Government Requests by Legal Process Type July 1–December 31, 2023

Tables 10, 11, 12, 13, and 14 provide information regarding United States requests by legal process type. Legal process types can be Search Warrants, Wiretap Orders, Pen Register/Trap and Trace Orders, Other Court Orders, or Subpoenas.

Table 10: United States Government Device Requests by Legal Process Type

Table 10 provides information regarding the types of legal process Apple received as Device Requests.

# of Device Requests	Search Warrants	Wiretap Orders	Pen Register/Trap & Trace Orders	Other Court Orders	Subpoenas
6,410	1,256	N/A	3	171	4,980
% of Total (100%)	19.6%	-	~0%	2.7%	77.7%

Table 11: United States Government Financial Identifier Requests by Legal Process Type

Table 11 provides information regarding the types of legal process Apple received as Financial Identifier Requests.

# of Financial Identifier Requests	Search Warrants	Wiretap Orders	Pen Register/Trap & Trace Orders	Other Court Orders	Subpoenas
1,018	199	N/A	0	34	785
% of Total (100%)	20%	-	-	3%	77%

Table 12: United States Government Account Requests by Legal Process Type

Table 12 provides information regarding the types of legal process Apple received as Account Requests.

# of Account Requests	Search Warrants	Wiretap Orders	Pen Register/Trap & Trace Orders	Other Court Orders	Subpoenas
10,827	5,493	2	92	597	4,643
% of Total (100%)	50.7%	~0%	0.8%	5.5%	42.9%

Table 13: United States Government Push Token Requests by Legal Process Type

Table 13 provides information regarding the types of legal process Apple received as Push Token Requests.

# of Push Token Requests	Search Warrants	Wiretap Orders	Pen Register/Trap & Trace Orders	Other Court Orders	Subpoenas
99	16	N/A	0	40	43
% of Total (100%)	16.2%	-	-	40.4%	43.4%

Table 14: United States Government Geofence Requests by Legal Process Type

Table 14 provides information regarding search warrants Apple received as Geofence Requests. Apple does not have any data to provide in response to geofence warrants.

# of Geofence Requests	Search Warrants	Wiretap Orders	Pen Register/Trap & Trace Orders	Other Court Orders	Subpoenas
11	10	N/A	N/A	N/A	1
% of Total (100%)	91%	-	-	-	9%

# of Device/ Financial Identifier/ Account/ Push Token Requests

The total number of United States government requests Apple received by request type (Device, Financial Identifier, Account, and Push Token). We count each individual request received from the United States by request type and report the total number of requests received by request type.

# of Geofence Requests

The total number of United States government requests Apple received seeking customer data related to specific latitude and longitude coordinates (geofence) for a specified time period. We count each individual request received from government agencies and report the total number of requests received. Apple does not have any data to provide in response to Geofence Requests.

Search Warrants

A search warrant is a judicial document used in a criminal case authorizing law enforcement officers to search a person or place to obtain evidence. The Fourth Amendment requires that law enforcement officers obtain search warrants by submitting affidavits and other evidence to a judge or magistrate to meet a burden of proof that a search will yield evidence related to a crime. The judge or magistrate will issue the warrant if satisfied that the law enforcement officers have met the burden of proof. For customer content, Apple requires a search warrant issued upon a showing of probable cause in order to provide content.

Wiretap Orders

A wiretap order is a specific type of court order used in a criminal case that authorizes law enforcement officers to obtain contents of communications in real-time. A Title III wiretap order includes requirements that law enforcement officers make an application and furnish evidence to a judge or magistrate to demonstrate there is probable cause to believe that interception of communications will yield evidence related to a particular crime, there is probable cause to believe that an individual has committed or is about to commit a particular crime and must specifically identify the individual/target whose communications are to be intercepted. A statement must also be included as to whether other investigatory measures have been tried and failed or are unlikely to succeed. If satisfied that the requirements have been met, the judge or magistrate will issue the wiretap order. A wiretap order allows the government to obtain content on a forward-looking basis for a specific limited period of time as opposed to stored historical content. Apple can intercept users' iCloud email communications upon receipt of a valid Wiretap Order. Apple cannot intercept users' iMessage or FaceTime communications as these communications are end-to-end encrypted.

Pen Register/Trap & Trace Orders

A pen register or trap and trace order is a specific type of court order used in a criminal case authorizing law enforcement officers to obtain headers of electronic communications and other non-content data in real-time. A pen register order requires law enforcement officers to make a statement of the offense to which the pen register relates and certify the information likely to be obtained is relevant/material to an ongoing criminal investigation. The legal standard for obtaining a pen register order is lower than what is required for a search warrant or a wiretap order. A pen register order allows the government to obtain non-content data on a forward-looking basis for a specific limited period of time as opposed to stored historical information. A pen register order can be combined with a court order/warrant for historical records; in such instances, we report the process type as pen register/trap and trace order.

Other Court Orders

A court order is a document issued by a judge or magistrate directing a person or entity to comply with the order. An order may be issued in either a criminal or civil case. Government agencies applying for an order in a criminal case must generally present facts and evidence to a judge or magistrate showing there are reasonable grounds to believe that the information sought is relevant and material to an ongoing criminal investigation or similar legal standard. Non-content data such as subscriber and transaction information can be provided in response to a court order.

Subpoenas

A subpoena or equivalent legal process request (e.g. petition or summons) is a document issued by a government agency or court directing a person or entity to comply with requests for information. Local, state and federal government agencies may issue subpoenas. Under many jurisdictions, a judge or magistrate is not required to review a subpoena before it is issued. Accordingly, the subpoena has the lowest threshold for burden of proof. A subpoena may be issued in either a criminal or civil case. Non-content data such as device, subscriber and connection information can be provided in response to a subpoena.

% of Total

The percentage of requests by Legal Process Type. We calculate this based on the number of respective Legal Process Types compared to the respective total number of Device/Financial Identifier/Account/Push Token Requests received by Apple.

Table 15: United States Private Party Requests for Information
July 1–December 31, 2023

Table 15 provides information regarding United States private party (non-government) requests for information. Examples of such requests are where private litigants are involved in either civil or criminal proceedings. Apple complies with these requests insofar as we are legally required to do so.

# of Private Party Requests	# of Requests Rejected/ Challenged & No Data Provided	# of Requests Where No Data Provided	# of Requests Where Data Provided
401	339	29	33
% of Total (100%)	85%	7%	8%

# of Private Party Requests

The number of requests received from private parties (non-government) in the United States seeking customer data related to specific devices, financial identifiers and/or accounts. We count each individual request received from private parties and report the total number of requests received.

# of Requests Rejected/ Challenged & No Data Provided

The number of private party requests that resulted in Apple challenging or rejecting the request based on grounds such as a request does not have a valid legal basis, or is unclear and/or over-broad; and where no data was provided. We count each private party request where we challenge or reject it in full, and report the total number of such instances.

# of Requests Where No Data Provided

The number of private party requests that resulted in Apple providing no data. For example, where there was no responsive data. We count each instance where we do not provide data in response to a private party request and report the total number of such instances.

# of Requests Where Data Provided

The number of private party requests that resulted in Apple providing data in response to valid legal process or subscriber consent. We count each instance where we provide data in response to a private party request and report the total number of such instances.

% of Total

The percentages are calculated based on the number of the respective response types compared to the total number of private party requests received by Apple.

Table 16: United States Private Party Requests for Account Restriction/Deletion July 1–December 31, 2023

Table 16 provides information regarding United States private party (non-government) requests for Apple account restriction/deletion. Examples of such requests are where private litigants are involved in either civil or criminal proceedings, and requests for Apple to restrict/delete an account may arise. For requests seeking to restrict/delete a customer's Apple ID, Apple requires a court order. Apple complies with these requests insofar as we are legally required to do so.

# of Account Restriction/ Account Deletion Requests Received	# of Accounts Specified in the Requests	# of Requests Rejected/ Challenged Where No Action Taken	# of Account Restriction Requests Where Account Restricted	# of Account Deletion Requests Where Account Deleted
0	0	0	0	0

# of Account Restriction/Account Deletion Requests Received

The number of requests received from private parties (non-government), such as participants in a civil or family law case, seeking to restrict or delete a customer's Apple ID. We count each individual request received from private parties and report the total number of requests received.

# of Accounts Specified in the Requests

The number of accounts specified in the requests. One request may contain one or multiple account identifiers. For example, in a case related to multiple shared accounts, a private party may request Apple to restrict or delete several accounts in a single request. We count the number of accounts identified in each request received from private parties and report the total number of accounts specified in requests received.

# of Requests Rejected/Challenged Where No Action Taken

The number of account restriction/deletion requests that resulted in Apple challenging or rejecting the request based on grounds such as a request does not have a valid legal basis, or is unclear, inappropriate, and/or over-broad, or where it is not accompanied by a court order demonstrating the grounds upon which the account is to be restricted/deleted; and where no action was taken by Apple. We count each account restriction/deletion request where we challenge or reject it and report the total number of such instances.

# of Account Restriction Requests Where Account Restricted

The number of account restriction requests where Apple determined the request and order sufficiently demonstrated the grounds upon which the specified account was to be restricted; and we proceeded with the requested restriction. We count each account restriction request where we proceeded with restriction and report the total number of such instances.

# of Account Deletion Requests Where Account Deleted

The number of account deletion requests where Apple determined the request and order sufficiently demonstrated the grounds upon which the specified account was to be deleted; and we deleted the Apple account. We count each account deletion request where we deleted an account and report the total number of such instances.

Table 17: Worldwide Government Digital Content Provider Requests July 1–December 31, 2023

Table 17 provides information regarding government requests received where digital content provider information is requested. Examples of such requests are where law enforcement agencies are investigating a digital content provider who may have provided a service or content (e.g. app, music item, or podcast) that is alleged/suspected to violate local law. These requests generally seek details of the content provider, such as name, email address, physical address, and in certain instances payment details or other information.

Country or Region[1]	# of Content Provider Requests Received	# of Content Provider Requests Objected to in Part or Rejected in Full	# of Content Provider Requests Where Data Provided	% of Content Provider Requests Where Data Provided
Asia Pacific				
China mainland	18	5	13	72%
Hong Kong	2	1	2	100%
Japan	3	1	3	100%
Macau	1	1	1	100%
Thailand	1	1	1	100%
Asia Pacific Total	25	9	20	80%
Europe, Middle East, India, Africa				
Germany	5	0	5	100%
Hungary	3	1	3	100%
India	6	3	4	67%
Latvia	1	1	1	100%
Spain	1	0	1	100%
United Kingdom	1	0	1	100%
Europe, Middle East, India, Africa Total	17	5	15	88%
Latin America				
Chile	1	1	0	0%
Latin America Total	1	1	0	-
North America				
Mexico	1	1	0	0%
United States of America	17	0	16	94%
North America Total	18	1	16	89%
Worldwide Total	61	16	51	84%

[1] Only countries / regions where Apple received digital content provider requests during report period July 1–December 31, 2023 are listed.

# of Content Provider Requests Received

The number of requests received from government agencies seeking digital content provider information related to specific digital content identifiers, such as digital asset ID, content provider ID, or digital content name. Requests can be in various formats such as subpoenas, court orders, warrants, or other valid legal requests. We count each individual request received from each country/region and report the total number of requests received by country/region.

# of Content Provider Requests Objected to in Part or Rejected in Full

The number of digital content provider-based requests that resulted in Apple objecting to or rejecting the request in part or in full based on grounds such as a request that does not have a valid legal basis, or is unclear, inappropriate, and/or over-broad. For example, Apple may reject a law enforcement request if it considers the scope of data requested to be excessively broad for the case in question. We count each digital content provider-based request where we object in part or reject in full and report the total number of such instances by country/region.

# of Content Provider Requests Where Data Provided

The number of digital content provider requests that resulted in Apple providing data, such as content provider name and contact information associated with a specific app, music item, or podcast, in response to a valid legal request. We count each digital content provider request where we provide data and report the total number of such instances by country/region.

% of Content Provider Requests Where Data Provided

The percentage of digital content provider requests that resulted in Apple providing data. We calculate this based on the number of digital content provider-based requests that resulted in Apple providing data per country/region, compared to the total number of digital content provider-based requests Apple received from that country/region.

Worldwide Government App Store Takedown Requests
January 1–December 31, 2023

Apple publishes government App Store takedown requests in a dedicated App Store Transparency Report that includes data showing takedown demands by government entity and law cited. See https://www.apple.com/legal/more-resources/.

Matters of note in this report:

Government requests related to customer data / accounts

Table 1 Worldwide Government Device Requests
China mainland - High number of devices specified in requests predominantly due to tax investigations.

Table 2 Worldwide Government Financial Identifier Requests
Taiwan - High number of financial identifiers specified in requests predominantly due to investigations involving Apple Gift Cards.

Clarifying Lawful Overseas Use of Data (CLOUD) Act Requests
Requests received pursuant to the U.S. CLOUD Act are included in Apple's transparency report. Apple received 120 CLOUD Act Investigatory Powers Act (IPA) Communications Data Requests (seeking metadata only) issued by the United Kingdom government in this reporting period. We count and report CLOUD Act requests under the country of origin.

Mutual Legal Assistance Treaty (MLAT) Requests
Requests received from a foreign government pursuant to the MLAT process or through other cooperative efforts with the United States government are included in Apple's transparency report. Apple identified 27 MLAT requests for information issued by the United States government in this reporting period. However, this may not be the precise number of MLAT requests received, as in some instances a United States court order or search warrant may not indicate that it is the result of an MLAT request. In instances where the originating country was identified, we count and report the MLAT request under the country of origin. In instances where the originating country was not identified, we count and report the request under the United States of America.